



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Amanda Harvey
Office: (267) 930-1697
Fax: (267) 930-4771
Email: aharvey@mullen.law

1452 Hughes Road, Suite 200
Grapevine, TX 76051

May 22, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent the Laborers Local No. 754 Joint Benefit Funds (the “Laborers Funds”) located at 215 Old Nyack Turnpike, Chestnut Ridge, New York 10977, and are writing to notify your office of an incident that may affect the security of certain personal information relating to seventeen (17) Maryland residents. This notice will be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, the Laborers Funds do not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about October 10, 2023, the Laborers Funds experienced malicious encryption that impacted certain servers utilized by the Laborers Funds. Upon identifying the activity, the Laborers Funds promptly worked to secure its systems and began an investigation, with the assistance of third-party cybersecurity specialists, to confirm the nature and scope of the event. The forensic investigation did not identify access to and/or exfiltration of sensitive information. However, out of an abundance of caution, the Laborers Funds are electing to provide notice and complimentary credit monitoring to potentially impacted individuals. The Laborers Funds engaged in a time intensive review of their systems to identify sensitive information within their network and to whom it related in order to provide notice out of an abundance of caution. This review was completed on or about May 7, 2024.

The information that could have been subject to unauthorized access includes name, Social Security number, financial account information, medical information, and health insurance information.

Notice to Maryland Residents

On or about May 22, 2024, Laborers Funds provided written notice of this incident to seventeen (17) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, the Laborers Funds moved quickly to investigate and respond to the incident, assess the security of Laborers Funds systems, and identify potentially affected individuals. Further, the Laborers Funds notified federal law enforcement regarding the event. The Laborers Funds are also working to implement additional safeguards and training to its employees. The Laborers Funds are providing access to credit monitoring services for twelve (12) months, through CyEx, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, the Laborers Funds are providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. The Laborers Funds are providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

The Laborers Funds are providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1697.

Very truly yours,

A handwritten signature in black ink, appearing to read "Amanda Harvey", followed by a horizontal line.

Amanda Harvey of
MULLEN COUGHLIN LLC

ANH/kzm
Enclosure

EXHIBIT A

Laborers Local No. 754 Joint Benefit Funds

Return Mail Processing
P.O. Box 2623
Duluth, GA 30096-9998

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

NOTICE OF <<SECURITY INCIDENT>> / [DATA BREACH]>>

Dear <<Name 1>> <<Name 2>>:

The Laborers Local No. 754 Joint Benefit Funds (“Laborers Funds”) write to inform you of an incident that may affect the privacy of some of your information. Although the Laborers Funds have not identified evidence of access, exfiltration, or attempted misuse of your information, we are providing you notice of the incident, steps we are taking in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On or about October 10, 2023, the Laborers Funds experienced malicious encryption that impacted certain servers utilized by the Laborers Funds. We promptly worked to secure our systems and began an investigation, with the assistance of third-party cybersecurity specialists, to confirm the nature and scope of the incident. The forensic investigation did not identify any access to and/or exfiltration of sensitive information related to our participants. We then engaged in a time intensive review of our systems to identify sensitive information within our network and to whom it related in order to provide notice out of an abundance of caution. This review completed on or about May 7, 2024.

What Information Was Involved? The information that the Laborers Funds may store on your behalf can include your name, <<Data elements>>. As noted above, the forensic investigation did not identify that any participant information was subject to unauthorized access and/or exfiltration.

What We Are Doing. The Laborers Funds take their responsibility to safeguard information seriously. As such, we responded promptly to this incident and worked diligently to provide you with an accurate and complete notice of the incident as soon as possible. As part of our ongoing commitment to the privacy and security of personal information in our care, we reviewed and updated existing policies and procedures relating to data protection and security. We also implemented additional security measures designed to mitigate risk and to limit the likelihood of future similar incidents. The Laborers Funds are providing notice of this incident to potentially impacted individuals and to regulators, where required.

Out of an abundance of caution, the Laborers Funds are providing you with <<12/24>> months of complimentary access to credit monitoring and identity restoration services through CyEx, as well as guidance on how to protect your information, should you feel it is appropriate to do so. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself.

What You Can Do. Although there is no evidence of any actual or attempted misuse of your information, the Laborers Funds encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and by monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. We also encourage you to review the information in the enclosed *Steps You Can Take to Protect Personal Information*. There, you will find additional information about the complimentary credit monitoring services and how to enroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call our dedicated assistance line at: 888-326-0989, Monday through Friday, 9:00 AM to 9:00 PM Eastern Time. You may also write to us directly at: 215 Old Nyack Turnpike, Chestnut Ridge, NY 10977.

Sincerely,

Laborers Local No. 754 Joint Benefit Funds

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

Identity Defense Complete

Enrollment Instructions

1. Visit app.identitydefense.com/enrollment/activate/llpw
2. Enter your unique Activation Code: <<Activation Code>>
3. Click 'Redeem Code'
4. Follow the prompts to create your account

The deadline to enroll is <<Deadline>>. After <<Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by <<Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 866.622.9303.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <#> Rhode Island residents that may be impacted by this event.